

УТВЪРДИЛ: Виолета Сидерова
Директор на ДГ № 4 „БРЕЗА „
Изготвил:адв. Елена Златева

Violeta
Zhelyazkova
Siderova

Digitally signed by
Violeta Zhelyazkova
Siderova
Date: 2025.09.16
11:05:02 +03'00'

ПРОЦЕДУРА ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ НА ДГ№ 4“ БРЕЗА“

Предназначение на процедурата

Всички дейности и проекти, осъществявани от ДГ, които предвиждат обработка на лични данни, са предмет на предварителна оценка на риска. Когато тази оценка покаже, че съществува вероятност обработването да породи висок риск за правата и свободите на субектите на данни, преди да извърши обработването, детското заведение извършва също и оценка на въздействието върху защитата на данните (ОВЗД) съгласно изискванията на тази процедура.

Освен при идентифициране на висок риск, ОВЗД се извършва задължително и в изброените в [член 35, параграф 3 от ОРЗД](#) случаи:

- когато се извършва систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;
- при мащабно обработване на „чувствителни“ лични данни или на лични данни за присъди и нарушения;
- при систематично мащабно наблюдение на публично достъпна зона.

ОВЗД е задължителна също и за видовете операции по обработване, посочени в списък, приет и оповестен от националния надзорен орган ([чл. 35, пар. 4 от ОРЗД](#)).

Нормативна уредба

- [Член 35](#) и [член 36](#) от Общия регламент за защита на данните (ОРЗД)
- [Насоки](#) относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за

целите на Регламент 2016/679¹

Задължения и роли

Директорът на детското заведение отговаря за извършването на необходимите проверки на личните данни, чиято цел е да се установи нуждата от провеждане на ОВЗД. Директорът може да възложи изпълнението на дейностите по прилагането и ефективното изпълнение на тази процедура на други служители с подходяща квалификация.

2

Лицата, ръководещи отделните процеси по обработка на данните в организацията, са отговорни за своевременното известяване на отговорното лице и за съвместното вземане на решения във връзка с възникнали рискове за сигурността на личните данни.

Ход на процедурата

1. Анализ на рисковете и оценка на въздействието

При започването на всяка дейност или проект отговорното лице извършва оценка на риска съгласно изискванията на настоящата процедура и определя дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679 на Работната група по чл. 29 от ОРЗД, като взема предвид вида на личните данни и начините за обработването им.

ОВЗД се извършва с цел определяне на адекватно ниво на технически и организационни мерки за защита на личните данни, което отговаря на обработваните от него лични данни и въздействието при нарушаване на защитата им. Оценката на въздействието е процес, при който администраторът преценява нивата на рисковете за правата и свободите на субектите на данни. Водещ критерий при тази преценка е степента (нивото) на въздействие, което нарушаването на поверителността, цялостността или наличността на личните данни би оказало върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица.

В съответствие с това, е необходимо да се анализира вероятността за възникване на нарушение на сигурността на данните и определя 4 нива на въздействие – ниско, средно, високо и изключително високо.

При извършването на ОВЗД, се използва следната матрица за степенуване на въздействието (риска), отчитаща вероятността за настъпване на съответното нарушение на сигурността на данните и величината на потенциалните неблагоприятни последици (вреди):

		Последици			
		Ограничени	Средни	Тежки	Много тежки
Вероятност	Малка	Ниско - 1 -	Средно - 4 -	Средно - 6 -	Високо - 10 -

	Средна	Ниско - 2 -	Средно - 5 -	Високо - 8 -	Изключително високо - 11 -
	Висока	Средно - 3 -	Високо - 7 -	Високо - 9 -	Изключително високо - 12 -

П

р
и

о
п

В зависимост от определеното ниво на въздействие, ДГ..... извършва:

Приоритизиране на идентифицираните рискове, и

е определя адекватно ниво на защита, включващо техническите и организационни мерки, които трябва да предприеме за тяхното преките рискове ограничаване.

Редът на **приоритизиране** на идентифицираните рискове е, както следва:

- 1) Рисковете с висока тежест на последиците и вероятност за настъпване (8, 9, 11 и 12) трябва да бъдат напълно избегнати или ограничени чрез прилагане на мерки за сигурност, които намаляват както тежестта им, така и тяхната вероятност. В плана за управление на рисковете следва да се предвидят както мерки за предотвратяване (действия, предприети преди вредно събитие), така и за защита (действия, предприети по време на вредно събитие) и възстановяване (действия, предприети след вредно събитие).
- 2) Рисковете с висока тежест, но с малка вероятност (6, 10) трябва да се избягват или ограничават чрез прилагане на мерки за сигурност, които намаляват тежестта на последиците или вероятността за настъпването им. **Приоритет следва да имат преди всичко на мерките за предотвратяване** (превантивните мерки).
- 3) Рисковете с малка тежест, но с голяма вероятност за настъпване (3, 7), трябва да бъдат ограничавани чрез прилагане на мерки за сигурност, които намаляват тяхната вероятност. **Трябва да се наблегне обаче на мерките за възстановяване.**
- 4) Рискове с ниска тежест и вероятност (1, 2, 4, 5) могат да бъдат третираны на по-късен етап, още повече че прилагането на мерките спрямо рисковете с по-висок приоритет може да доведе до тяхното елиминирание или значително ограничаване.

На следващо място, в зависимост от приоритизацията на рисковете и идентифицираното ниво на въздействие, ДГ..... определя съответно ниво на защита – ниско, средно, високо или изключително високо, както и организационните и технически мерки, адекватни на така

р
и
с
к
а

определеното ниво.

Минималното необходимото съдържание на ОВЗД [/член 35, параграф 7 от ОРЗД/](#), е:

- системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
- оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
- оценка на рисковете за правата и свободите на субектите на данни; и
- мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на ОРЗД.

След консултация с Длъжностното лице по защита на данните ДГодобрява и подписва ОВЗД за всяка подлежаща на оценка на въздействието дейност.

Освен при започване на нова дейност/проект,ДГ..... прави преглед за необходимостта от извършване на оценка на въздействието и при всяка промяна в риска, с който са свързани вече съществуващи операции по обработване ([член 35, параграф 11 от ОРЗД](#)). ОВЗД следва постоянно да се преразглежда и да подлежи на редовна повторна оценка. Пълният цикъл на повтарящия се процес на извършване на ОВЗД е онагледен в [Насоките](#) на Работната група по член 29 със следната илюстрация:



2. Записи в Регистъра на дейностите по обработване

ДГ..... записва информация за всички лични данни, включително разпознатите като „рискови“, обработвани в рамките на всяка отделна дейност/проект, и за всички процеси, свързани с тази дейност/проект в Регистъра на дейностите по обработване. Това включва описание на обработката и целите за които се извършва, законоустановените интереси, преследвани от администратора, оценка на необходимостта и пропорционалността на обработката на данните, категорията на данните (обща, специална, отнасящи се до дете), формата на данните, оценка на рисковете за правата и свободите на субектите на данни (съгласно схемата и определенията за нивото на въздействие, посочени по-горе). В Регистъра на дейностите по обработване се вписват също така всички видове операции по обработката на данните – събиране, прехвърляне, съхранение, достъп, изтриване. След извършването на ОВЗД, в Регистъра на дейностите по обработване са вписват данни и за определеното адекватно ниво на защита и набелязаните организационни и технически мерки за елиминиране или ограничаване на рисковете.

С оглед на идентифицираното основание за обработка на данните, ДГ..... определя и записва в Регистъра на дейностите по обработване съответния период на съхранение .

Организацията определя и посочва в Регистъра на дейностите по обработване кои лица имат достъп до данните (физически лица, работни екипи, организационни звена, трети лица) и/или кои лица участват в обработката на личните данни.

3. Предварителна консултация

Когато в резултат на извършена ОВЗД преди започването на обработката на лични данни ДГ..... установи, че обработката им ще доведе до висок риск за субектите на данни и че не е могъл да идентифицира адекватни мерки за ограничаване и контрол на риска, организацията се консултира с надзорния орган (за България КЗЛД) съгласно изискванията на [чл. 36 от ОРЗД](#).

Когато поиска консултация от надзорния орган, ДГ..... му предоставя следната информация:

- информация за съответните отговорности на администратора, съвместните администратори и обработващите лични данни, които се занимават с обработването, по-конкретно при обработването на данни в рамките на група предприятия;
- целите на планираното обработване и средствата за него;
- предвидените мерки и гаранции за защита на правата и свободите на субектите на данни;
- координатите за връзка на длъжностното лице по защита на данните;
- копие от ОВЗД, както и
- всякаква друга информация, поискана от надзорния орган.

УТВЪРДИЛ:

Директор:.....